

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-157585

(43)Date of publication of application : 29.05.1992

(51)Int.Cl.

G06K 17/00

(21)Application number : 02-282035

(71)Applicant : TOSHIBA CORP
TOSHIBA INTELLIGENT TECHNOL LTD

(22)Date of filing : 22.10.1990

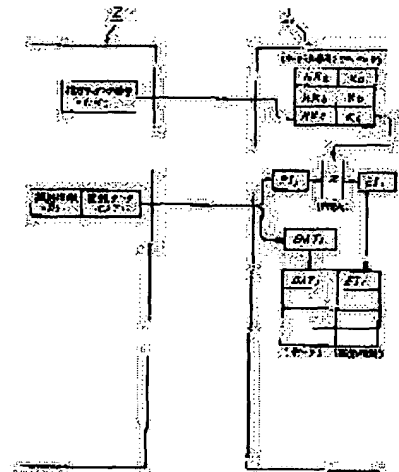
(72)Inventor : NIIMURA TAKASHI

(54) INFORMATION MANAGEMENT SYSTEM

(57)Abstract:

PURPOSE: To improve data security by disenabling an access to data stored in the data memory of an IC card with any equipment other than a legal host device (host computer).

CONSTITUTION: A second electronic device (host computer) 2 performs data management by assigning identification information to each data. When the second electronic device 2 accesses the storage means of a second electronic device (IC card) 1, when prescribed key data are designated from among several key data Ka to Kc preliminarily stored in the first electronic device 1 by the second electronic device 2, the identification information assigned to each data is coded by using the key data. Each data is assigned with the coded identification information and the access to each data stored in the first electronic device 1 is executed based on the coded identification information. Thus, the security for the data stored in the first electronic device can be improved.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

平4-157585

⑬ Int. Cl.³

G 06 K 17/00

識別記号

S
E

庁内整理番号

6711-5L
6711-5L

⑭ 公開 平成4年(1992)5月29日

審査請求 未請求 請求項の数 1 (全8頁)

⑮ 発明の名称 情報管理方式

⑯ 特 願 平2-282035

⑰ 出 願 平2(1990)10月22日

⑱ 発 明 者 新 村 貴 志 神奈川県川崎市幸区柳町70番地 東芝インテリジェントテクノロジー株式会社内

⑲ 出 願 人 株 式 会 社 東 芝 神奈川県川崎市幸区堀川町72番地

⑲ 出 願 人 東芝インテリジェントテクノロジー株式会社 神奈川県川崎市幸区柳町70番地

⑳ 代 理 人 弁理士 則近 憲佑 外1名

明 細 書

1. 発明の名称

情報管理方式

2. 請求の範囲

複数のデータと、複数のキーデータとを記憶する記憶手段を有してなる第1の電子装置と、前記第1の電子装置の記憶手段に記憶されているデータの各々に対して識別情報を与える手段を有してなる第2の電子装置とからなり、前記第2の電子装置は前記識別情報に基づいて前記第1の電子装置の記憶手段に記憶されている所定のデータにアクセスするものであって、前記第1の電子装置に設けられた記憶手段中に記憶されている複数のキーデータのうち、前記第2の電子装置により指定されたキーデータを用いて前記識別情報を暗号化する手段を具備してなり、前記第1の電子装置に記憶されている所定のデータへのアクセスは、前記暗号化された識別情報に基づいて行われることを特徴とする情報管理方式。

3. 発明の詳細な説明

【発明の目的】

(産業上の利用分野)

本発明は、例えばホストコンピュータ等の上位装置から送信され、不揮発性メモリおよびCPUなどの制御素子を有するIC(集積回路)チップを内蔵したICカードと称される携帯可能記憶媒体に記憶されたデータを管理する情報管理方式に関する。

(従来の技術)

従来、携帯可能なデータ記憶媒体としてEEPROMなどのデータメモリ及びCPUなどの制御素子を有するICチップを内蔵したICカードが考えられている。この種のICカードは内蔵する制御素子によってデータメモリにアクセスし、外部(上位装置)からの要求に応じて必要なデータの入出力を選択的に行うようになっている。このICカードにホストコンピュータから送られたデータはデータメモリ中に順次記憶されていくものである。

ここで前記データメモリ中に記憶されたデー

タに対するアクセスを容易に行う方法として記憶されており、各データに独自の識別情報を与える方法が考えられている。

識別情報とは例えばデータメモリに記憶された順序を表す数値であり、第11図に見られるように5つのデータがデータメモリ10内でA、B、C、D、Eの順列で格納されている場合、「識別情報2のデータ」とはBであり、「識別情報4のデータ」とはDである。今、ホストコンピュータ側から「識別情報2のデータ」の読出命令を受信すると、ICカード内の制御素子はデータメモリ10内の上位から2番目に格納されているデータ（第10図の例ではB）を読出し、そのデータの内容をホストコンピュータへと送信するものである。

このような情報管理方式においては、使用者は例えばパスワード等をホストコンピュータを通して入力し、これにより正当な使用者であると認識されればICカードに対してデータの読み書きを行うことができる。

記憶する記憶手段を有してなる第1の電子装置と前記第1の電子装置の記憶手段に記憶されているデータの各々に対して識別情報を与える手段を有してなる第2の電子装置とからなり、前記第2の電子装置は前記識別情報に基づいて前記第1の電子装置の記憶手段に記憶されている所定のデータにアクセスするものであって、前記第1の電子装置に設けられた記憶手段中に記憶されている複数のキーデータのうち、前記第2の電子装置により指定されたキーデータを用いて前記識別情報を暗号化する手段を具備してなり、前記第1の電子装置に記憶されている所定のデータへのアクセスは、前記暗号化された識別情報に基づいて行われることを要とする。

(作用)

第2の電子装置（ホストコンピュータ）は各データに識別情報を付してデータ管理を行っている。この第2の電子装置から第1の電子装置（ICカード）の記憶手段に対してアクセスを行う場合には、まず第2の電子装置は第1の電子装置に

(2) ところが、前記パスワード照合等の所定の前処理さえ正に終了していれば、どんなホストコンピュータからでも、ICカード内に記憶されているデータに対するアクセスを容易に行うので、データのセキュリティが不十分であった。

(発明が解決しようとする課題)

上述したように従来の識別情報を用いた情報管理方式では、ICカードのデータメモリ内に記憶されたデータに対するアクセスが、どの上位装置からでも簡単に行えるので、データのセキュリティが不十分であるという問題点があった。

そこで本発明は、正当な上位装置（ホストコンピュータ）でなければICカードのデータメモリに記憶されているデータに対してアクセスできないような、データのセキュリティが充分な情報管理方式を提供することを目的とする。

[発明の構成]

(課題を解決するための手段)

上記目的を達成するために、本発明の情報管理方式は、複数のデータと複数のキーデータとを

あらかじめ記憶されている複数のキーデータの中から、所定のキーデータを指定する。次に、このキーデータを用いて、各データに与えられている識別情報が暗号化される。そして、各データには、この暗号化された識別情報が付与され、第1の電子装置に記憶された各データへのアクセスは、暗号化された識別情報に基づいて行われる。

(実施例)

以下、本発明をICカードとホストコンピュータとからなるシステムに適用した一実施例を、図面を参照して説明する。

第3図はICカード1とホストコンピュータ2とからなるシステムの構成例を示すものである。このICカード1は制御部としての制御素子3（例えばCPU）を含む。そして、この制御素子3によりデータメモリ4、プログラムメモリ5及びコンタクト部6が制御されている。このうち、データメモリ4は各種データの記憶に使用され、例えばEEPROMで構成されている。また、プログラムメモリ5は、例えばマスクROMで構成

されており、制御素子3の制御プログラムなどを記するものである。コンタクト部6は、後述するホストコンピュータ2のカードリーダーライタ8との電気的接触を得るためのものである。ここで破線内の部分、制御素子15、データメモリ16、プログラムメモリ17は1つのICチップで構成されてICカード本体内に埋設されている。さて、ホストコンピュータ2側も、例えばCPUからなる制御部7を有する。そして、この制御部8によって、カードリーダーライタ8、キーボード9、CRTディスプレイ10が制御されている。このうち、カードリーダーライタ8は前述したICカード1に対してデータの書き込み、読出し等を行うものである。また、キーボード9は例えば、制御部7に対する指示を入力したり、ICカード1に書き込むデータを入力したりするための入力手段である。CRTディスプレイ10は、カードリーダーライタ8を通して読出されたICカード1のデータメモリ4の内容を表示したり、何らかのエラーが発生した場合にエラーメッセージを表示したりするた

スワードが入力されると、ICカード1に対するアクセスが許可される(Step3)。ここで、正当でないパスワードが入力されたなら、その旨のエラー表示がCRTディスプレイ10上に表示され(Step4)、例えばもう一度パスワードの入力を促す。次に制御部7はICカード1のプログラムメモリ5中に記憶されているキーデータのキーデータ番号の中から、所定のキーデータ番号NKcを指定する(Step5)。ここで、どのキーデータ番号を指定するかはホストコンピュータ2の制御部7によって予め定められている。続いて、このキーデータ番号NKcに対応しているキーデータKcがプログラムメモリ5中で検索される(Step6)。そして指定されたキーデータ番号NKcが存在しない場合は、その旨のエラー表示をCRTディスプレイ10上に表示し(Step7)処理を終了する。

以上の処理が正常に終了するとホストコンピュータ2は、読みを行うデータDAT1に与えられている識別情報P11と書き込みを行うデータD

(3) めの表示手段である。

ここで、前記ICカード1のプログラムメモリ5内には、後述する「識別情報」を暗号化するのに使用される「キーデータ」があらかじめ複数個記憶されている。これら「キーデータ」の各々には、それぞれ独自の「キーデータ番号」が付与されており、「キーデータ」と「キーデータ番号」とは対応づけられて記憶されている。また、ホストコンピュータ2の制御部7は、データをICカード1に対して書き込む際、各データに独自の「識別情報」を付与し、この「識別情報」に基づいて各データを管理している。ここで、この「識別情報」は各データと一対一に対応している。

いま、ホストコンピュータ2からICカード1に対してデータの書き込みを行う場合の動作について第1図及び第2図を用いて説明する。まず、オペレータがホストコンピュータ2に設けられたキーボード6を通じてパスワードを入力し(Step1)、制御部7はこのパスワードが正当なものかどうかを判断する(Step2)。正当なパ

スワードを入力されると、ICカード1に対して送信する(Step8)。次にホストコンピュータ2から識別情報P11を受け取ったICカード1では、先にホストコンピュータ2によって指定されたキーデータKcを用いて制御素子3が前記識別情報P11を暗号化し、暗号化識別情報E11を生成する処理が行われる(Step9)。続いてICカード1のデータメモリ4内に暗号化識別情報E11と、これに対応するデータDAT1が記録される(Step10)。このとき、データメモリ4内では第4図に示されるようにデータは暗号化識別情報に連続して記憶され「暗号化識別情報、データ、暗号化識別情報、データ、…」のように隙間なく詰めて記憶されている。更にデータの先頭には該データのデータ長を表す情報(図示しない)が付加されて記憶される。

次に以上のような動作によって書き込まれたデータを読出す処理について第5図及び第6図を用いて説明する。

ここで、データの読出し処理において、パス

ワード入力から指定キーデータの検索までの動作 (Step 1 から Step 7 までの動作) は先に説明したデータの書き込み処理における動作と共通であるので、説明を省略する。さて、次に、オペレータは読出しを行うデータ D A T 1 の識別情報 P 1 1 をキーボード 9 等からの入力により指定する (Step 8)。続いて、先に指定されたキーデータ K c を用いて、ホストコンピュータ 2 側の制御部 7 が、前記識別情報 P 1 1 を暗号化し、暗号化識別情報 E 1 1 が生成される (Step 9)。そして、この暗号化された識別情報 E 1 1 が I C カード 1 に対して送信される (Step 10)。一方 I C カード 1 側では、制御素子 3 がデータメモリ 4 内の暗号化識別情報を次々と検索してゆき該当する暗号化識別情報がデータメモリ 4 内に存在するかどうかを判断する (Step 11)。ここで、該当する暗号化識別情報 E 1 1 がデータメモリ 4 内に存在する場合、該データメモリ 4 内で、該暗号化識別情報 E 1 1 の直後に格納されているデータ D A T 1 の読出しが行われ (Step 12)

識別情報 E 1 3 ではないので、次の暗号化識別情報を検索する。このとき、暗号化識別情報 E 1 1 のデータ D A T 1 のデータ長を参照して、該データ長分ジャンプすることによって、次の暗号化識別情報を認識する。このようにして制御素子 3 はデータメモリ 4 内で次々と暗号化識別情報を検索していく。そして処理対象データ D A T 3 の暗号化識別情報 E 1 3 が認識されるとそれに連続して格納されているデータ D A T 3 に対して消去する処理を行う。このとき、制御素子 3 はデータ D A T 3 のデータ長を参照して、データ D A T 3 自体を消去するとともに、このデータ D A T 3 に付与されていた暗号化識別情報 E 1 3 も同時に消去する。そしてデータ D A T 3 及び暗号化識別情報 E 1 3 が格納されていた領域は未使用領域となる。こうして、データ D A T 3 が消去された後のデータメモリ 4 内の様子を第 8 図に示す。

いま、ホストコンピュータ 2 から I C カード 1 に対して識別情報 P 1 6 とデータ D A T 8 とが送信されてきたとする。この識別情報 P 1 6 は前

(4)、このデータ D A T 1 がホストコンピュータ 2 側に送信される (Step 13)。前記 Step 11 において、ホストコンピュータ 2 から送信されてきた暗号化識別情報 E 1 1 が I C カード 1 のデータメモリ 4 内に存在しない場合は、「該当するデータは存在しない」旨のエラーメッセージをホストコンピュータ 2 に送信して (Step 14)、読出し処理を終了する。

次に、データメモリ 4 内の様子を参照して、データの読出し動作について説明する。今、第 7 図に見られるように 5 つのデータ D A T 1、D A T 2、D A T 3、D A T 4、D A T 5 がデータメモリ 4 中に記憶されており、これらデータには暗号化識別情報 E 1 1、E 1 2、E 1 3、E 1 4、E 1 5 がそれぞれ与えられているものとする。ここで、暗号化識別情報 E 1 3 のデータ D A T 3 を消去する処理について説明する。制御素子 3 はデータメモリ 4 内の上から順に暗号化識別情報を検索していく。まず、最初に制御素子 3 は暗号化識別情報 E 1 1 を認識するが、処理対象の暗号化識

別情報 E 1 3 ではないので、暗号化識別情報 E 1 3 となる。一方、制御素子 3 は、データメモリ 4 中を先頭から検索し、最初に存在する未使用領域に暗号化識別情報 E 1 3 及びデータ D A T 3 とを格納する。ここで、最初に存在する未使用領域に暗号化識別情報 E 1 3 及びデータ D A T 3 が格納しきれなかった場合、制御素子 3 は例えば第 9 図に見られるように、次に存在する未使用領域を検索し、データ D A T 3 を分割して格納する。このとき、分割されたデータ D A T 3 - 1 の末尾には、これに連続するデータ D A T 3 - 2 がデータメモリ 4 内のどこに格納されたかを表す連続情報 1 1 が付加される。この連続情報 1 1 は例えばデータ D A T 3 - 2 の先頭アドレスが記録されている。

また、データメモリ 4 中にすでに格納されているデータ群の末尾に新たなデータを追加記録する場合について説明する。例えば第 7 図に示すようにデータメモリ 4 内に 5 つのデータ D A T 1、D A T 2、D A T 3、D A T 4、D A T 5 が格納されており、それぞれのデータの暗号化識別情報

(5)

がE11、E12、E13、E14、E15であるとする。今、新たなデータとしてデータD A T 8を追加格納する。このデータD A T 8の識別情報P I 8は暗号化されて暗号化識別情報E I 8となる。そして、制御素子1がデータメモリ4内の未使用領域を検索して、検索された未使用領域に暗号化識別情報E I 8ならびにデータD A T 8を格納する。このときのデータメモリ4内の様子を第10図に示す。データD A T 8を格納するための未使用領域がデータメモリ4内に存在しなかった場合は、「メモリがいっぱいである」旨のメッセージをホストコンピュータ2に送信して処理を停止する。

以上詳述したように本実施例では、ホストコンピュータによって指定されたキーデータによってデータの識別情報を暗号化し、この暗号化された識別情報を用いてI Cカードに記憶されるデータの管理が行われる。このため、キーデータを正しく指定できないホストコンピュータからは、I Cカードに記憶されているデータの正しい識別情

報を指定することができない。即ち、正当なホストコンピュータしか、I Cカードに記憶されているデータに対してのアクセスを行えないので、データのセキュリティが高められる。更に、データ自身を暗号化することなく、識別情報のみを暗号化するので、制御素子(C P U)の負担を小さくできる。

また、I Cカードに記憶される各データに与えられる暗号化識別情報は絶対的な値であり、それぞれが独立している。そのため、一度、暗号化識別情報が与えられると該暗号化識別情報とデータとの対応が変化しないので、データ管理を容易に行うことができる。

なお、以上説明した実施例では、データ書込時にはI Cカード1側で識別情報の暗号化を行い、既にI Cカード1のデータメモリ4内に格納されているデータに対して処理を行う場合(以下データ処理時と称する)には、ホストコンピュータ2側で、識別情報の暗号化を行う。ここで、データを書込む際にはホストコンピュータ2側で識別情

報の暗号化を行い、書込まれたデータ进行处理する際にはI Cカード1側で識別情報の暗号化を行うものであってもよい。また、データ書込時においても、データ処理時においても、識別情報の暗号化をホストコンピュータ2側で行うものであってもよい。更に、また、データ書込時においても、データ処理時においても、識別情報の暗号化をI Cカード1側で行うものであってもよい。

また、本実施例中では、キーデータ番号並びにキーデータは、予めI Cカードのプログラムメモリ5中に格納されているものであったが、キーデータ番号並びにキーデータがデータメモリ4中のある領域に格納されるものであってもよい。

【発明の効果】

上述したように、本発明の情報管理方式によれば、正しいキーデータを指定することのできる正当な第2の電子装置(ホストコンピュータ)のみによってしか第1の電子装置(I Cカード)に格納されてい データに対するアクセスは行いえず、第1の電子装置に格納されているデータのセ

キュリティが高められる。

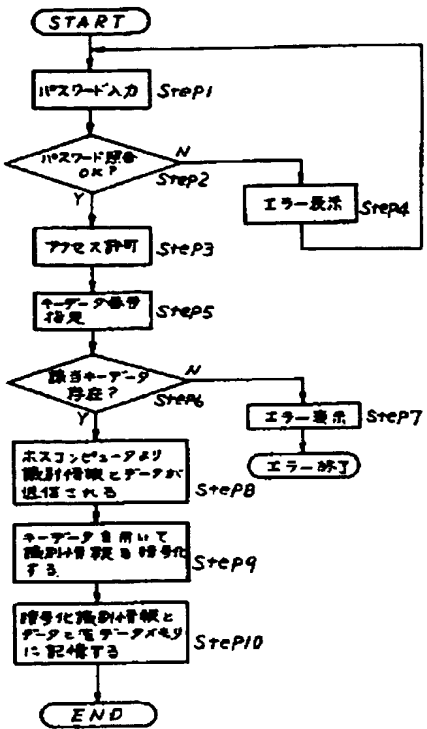
4. 図面の簡単な説明

第1図乃至第9図は本実施例を説明するためのもので、第1図はデータ書込み処理を行う場合のフローチャート、第2図はデータ書込み処理を行う場合のI Cカードとホストコンピュータ間のデータの授受を説明するための図、第3図はデータメモリ中の様子を説明するための図、第4図はデータ読出し処理を行う場合のフローチャート、第5図はデータ読出し処理を行う場合のI Cカードとホストコンピュータ間のデータの授受を説明するための図、第6図はデータメモリ内の記憶データ例を示す図、第7図はデータD A T 8を消去した後のデータメモリ内の様子を示す図、第8図はデータメモリ中の未使用領域に新しいデータを挿入した場合のデータメモリ内の様子を示す図、第9図はデータを分割格納したときのデータメモリ内の様子を示す図、第10図は新たなデータを追加格納したときのデータメモリ内の様子を示す図、第11図は従来例を説明するための図である。

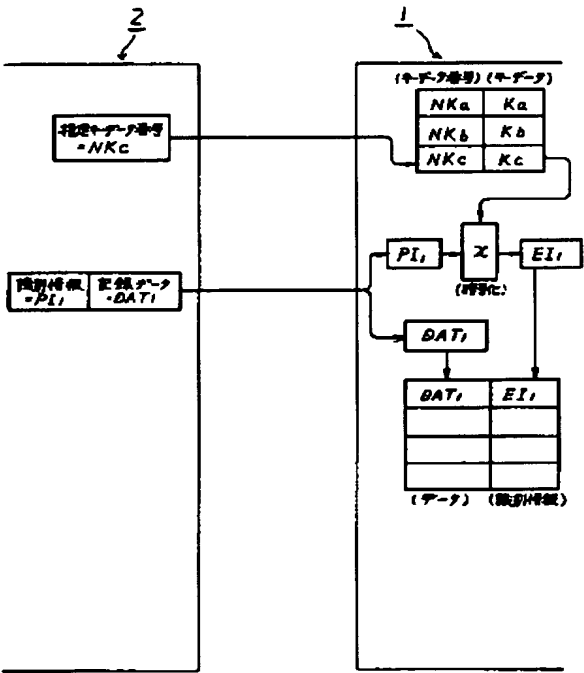
(6)

- 1 ... IC カード
- 2 ... ホストコンピュータ
- 3 ... 制御素子
- 4 ... データメモリ
- 5 ... プログラムメモリ

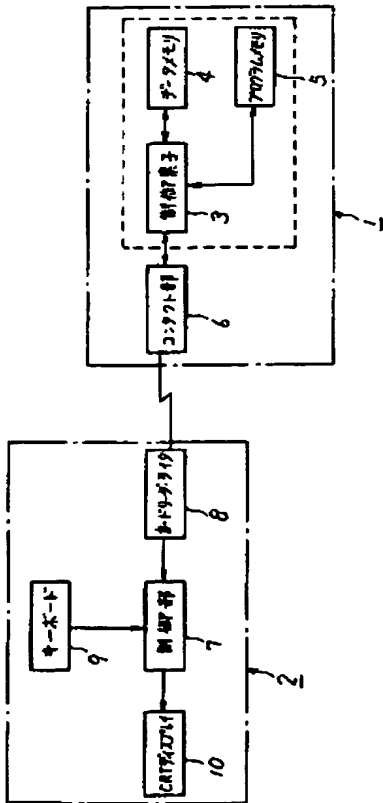
代理人 弁理士 則 近 憲 佑
同 山 下 一



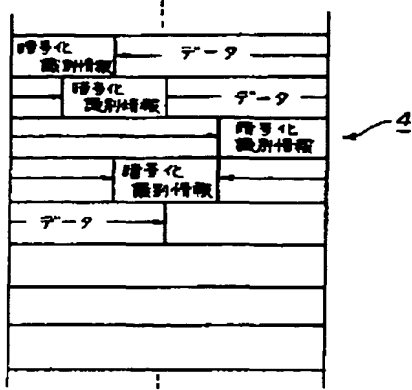
第 1 図



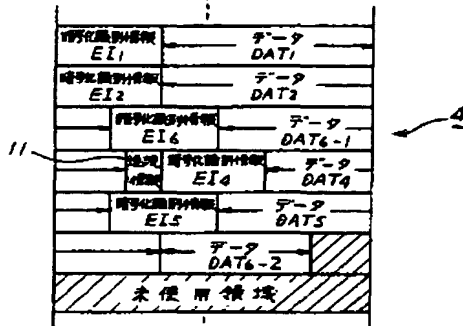
第 2 図



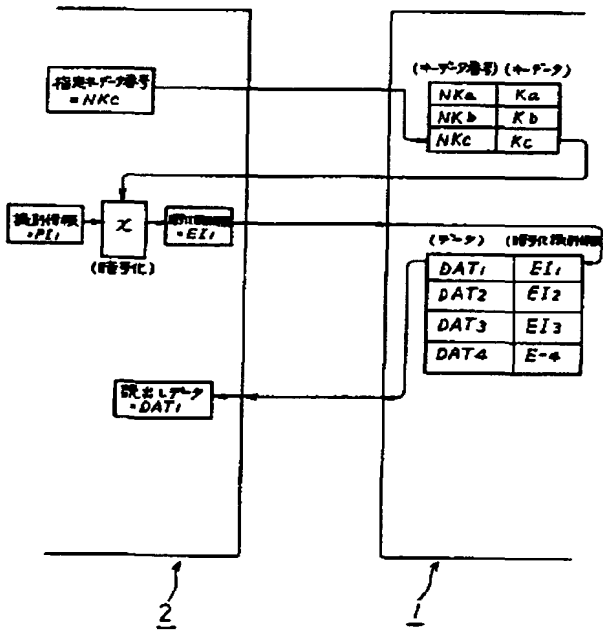
第 3 図



第 4 図

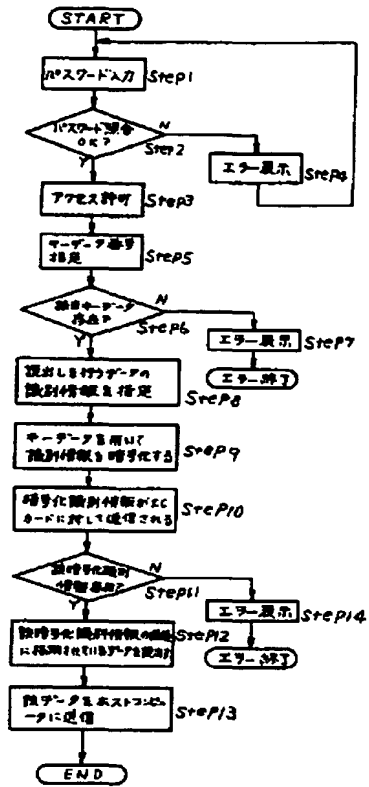


第 9 図

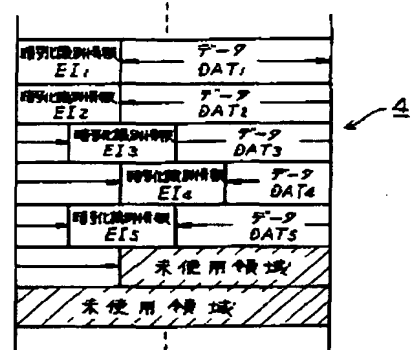


第 6 図

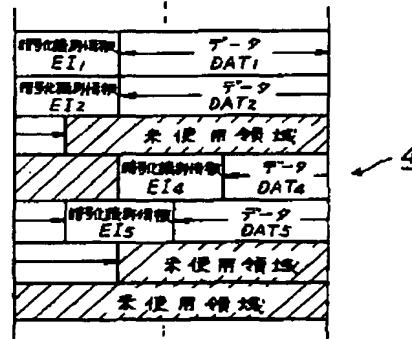
(7)



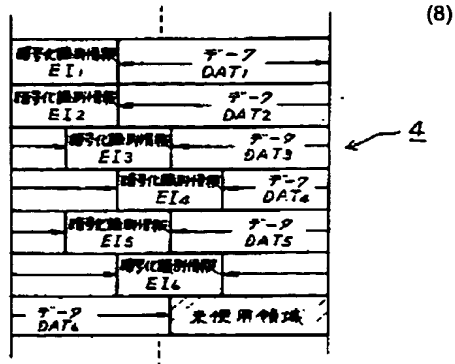
第 5 図



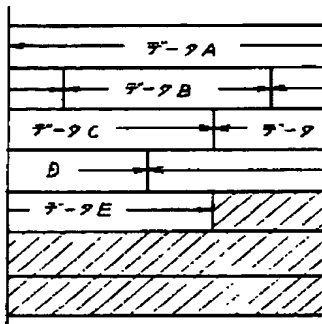
第 7 図



第 8 図



第 10 図



第 11 図